

AMENDMENTS TO THE SPECIFICATION

Please replace the paragraph at page 1, lines 8-17, with the following amended paragraph:

FIG. 1 is a diagram of a related art communication system, for example, an Internet system, for Digital Rights Management (DRM). User computers 10a . . . 10d, a content providing server 141, a key-data management server 142, and a payment system 143 are connected to one another through a communication network 12. The content providing server 141 provides content to the user computers 10a . . . 10d and receives charges related to DRM through the payment system 143. The key-data management server 142 manages key-data for encrypting and decrypting content files, which the content providing server 141 provides to the user computers 10a . . . 10d.

Please replace the paragraph at page 4, line 21 - page 5, line 2, with the following amended paragraph:

Also, a content file is provided that comprises a header portion having key-data for ~~digital right management~~ Digital Rights Management (DRM) information and DRM information distributively stored in a plurality of predetermined places of a hard disc, and a data portion.

Please replace the paragraph at page 5, lines 7-8, with the following amended paragraph:

FIG. 1 is a diagram of a related art communication network system for Digital Rights Management (DRM);

Please replace the paragraph at page 5, lines 11-12, with the following amended paragraph:

FIG. 3 is a block diagram of the structure of a content file according to an ~~preferred~~ embodiment of the present invention;

Please replace the paragraph at page 5, lines 16-18, with the following amended paragraph:

FIG. 5 is a flowchart of a first ~~preferred~~ embodiment of a program performed by a user computer to securely manage DRM information of the content file of FIG. 3; and

Please replace the paragraph at page 5, lines 19-21, with the following amended paragraph:

FIG. 6 is a flowchart of a second ~~preferred~~ embodiment of a program performed by a user computer to securely manage DRM information of the content file of FIG. 3.

Please replace the section heading at page 6, line 1, with the following amended section heading:

DETAILED DESCRIPTION OF ~~THE INVENTION~~ EXEMPLARY EMBODIMENTS

Please replace the paragraph at page 6, lines 2-11, with the following amended paragraph:

FIG. 3 illustrates a content file according to ~~an preferred~~ embodiment of the present invention that includes a header 41 and data 42. The header 41 includes encryption information EI, user key-data KU, key-data KS for synchronizing information, key-data KD for Digital Rights Management (DRM) information, synchronizing information SI, and DRM information, which is important information for a user. In the present invention, “important information” is defined to include, but is not limited to, DRM information that indicates a number of use times permitted to a user, so as to enable effective performance of DRM.

Please replace the paragraph at page 6, lines 12-23, with the following amended paragraph:

In the header 41, the encryption information EI contains parameters used for encrypting the data 42 of the content file, and the user key-data KU is used for encrypting and decrypting the data 42 of the content file. Also, the key-data KS for synchronizing information is used for encrypting and decrypting the synchronizing information SI, and the key-data KD for DRM

information is used for encrypting and decrypting the DRM information. The synchronizing information SI is continuously updated to determine whether the important DRM information has been hacked. In an ~~preferred~~ embodiment of the present invention, the synchronizing information SI can be embedded in the DRM information. ~~The important~~ Important DRM information indicates, for example, the number of use times permitted to a user, but is not limited thereto.

Please replace the paragraph at page 7, lines 1-19, with the following amended paragraph:

FIG. 4 illustrates the encrypted synchronizing information SI, which is distributively stored in predetermined places SI1, SI2, and SI3, for example. For example, but not by way of limitation, if an information managing method according to the present invention is applied only to the user computer 10a of FIG. 1 (here, the important information will not be the DRM information DRM of FIG. 3), the encrypted synchronizing information SI is distributed and stored in predetermined places of a hard disc drive. In this case, when the information managing method is applied to a communication network system as shown in FIG. 1, the encrypted synchronizing information SI may be distributed and stored in the key-data management server 142. Since the encrypted synchronizing information SI is distributed and stored in predetermined places, the risk of exposing the encrypted synchronizing information SI is minimized. According to this principle, the synchronizing information SI and the key-data KS for synchronizing information of FIG. ~~[[2]]~~3 are distributed and stored in predetermined places

according to a method shown in FIG. 5. The important DRM information DRM and the key-data KD for DRM information can be distributed and stored in predetermined places according to a method shown in FIG. 6.

Please replace the paragraph at page 7, line 20 - page 8, line 2, with the following amended paragraph:

FIG. 5 shows a first ~~preferred~~ embodiment of a program performed by the user computer 10a of FIG. 1 to securely manage the important DRM information DRM of the content file of FIG. 3. In the program of FIG. 5, the important DRM information DRM is not encrypted, so the DRM information key-data KD of FIG. 3 is not necessary.

Please replace the paragraph at page 8, line 20 - page 9, line 2, with the following amended paragraph:

If the synchronizing information decrypted in step S502 is the same as the synchronizing information decrypted in step S503, then ~~in step S504~~[[,]] update of the important DRM information DRM is monitored in step S508. The update of the DRM information DRM is related to, for example, the number of uses of the data 42 of the content file of FIG. 3.

Please replace the paragraph at page 9, lines 3-11, with the following amended paragraph:

If the DRM information DRM has been updated, new synchronizing information and important DRM information DRM is stored in the database in step S509. Next, the synchronizing information SI stored in the database is encrypted in step S510. Next, key-data KS for the encrypted synchronizing information SI is encrypted in step S511. Sequentially, the encrypted synchronizing information and key-data ~~[[is]]~~ are distributed and stored in predetermined places in step S512. Steps S508 through S512 are repeated until a termination signal is input in step S513.

Please replace the paragraph at page 9, lines 12-16, with the following amended paragraph:

FIG. 6 shows a second ~~preferred~~ embodiment of a program performed by the user computer 10a of FIG. 1 to securely manage the important DRM information DRM of the content file of FIG. 3. In the program of FIG. 6, the important DRM information DRM is encrypted, so the DRM information key-data KD of FIG. 3 is used.

Please replace the paragraph at page 10, line 16 - page 11, line 6, with the following amended paragraph:

If the information is the same in step S604, update of the important DRM information DRM is monitored in step S608. The update of the DRM information DRM is related to, for example, the number of uses of the data 42 of the content file of FIG. 3. If the DRM information DRM has been updated, new synchronizing information and important DRM information DRM is stored in the database in step S609. Next, the synchronizing information SI and the important DRM information DRM of FIG. 3 stored in the database are encrypted in step S610. Next, key-data KS for the encrypted synchronizing information SI and key-data KD for the important DRM information DRM are encrypted in step S611. Sequentially, the encrypted synchronizing information, important DRM information, and key-data are distributed and stored in predetermined places in step S612. Steps S608 through S612 are repeated until a termination signal is input in step S613.